

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-16. (Canceled)

17. (Currently amended) ~~The~~ An optical disk player according to claim 20, wherein the playing system comprising:

downloadable content provided on one or more computing devices distributed on a network, the downloadable content being associated with media content;

an optical disk comprises digital information stored thereon,  
~~the stored digital information comprising,~~ stored media content  
that is played in coordination with the downloadable content  
associated with the stored media content; and

a public key which is used ~~by the optical disk playing system~~  
to verify the authenticity of the downloadable content before the  
stored media content is played in coordination with the associated  
downloadable content.

18. (Currently amended) The optical disk ~~player~~playing system according to claim 17, wherein the public key is stored in a BCA (Burst Cutting Area) zone of the optical disk.

19. (Currently amended) The optical disk ~~player~~playing system according to claim 17, wherein the public key is stored in a media content zone of the optical disk.

20. (Currently amended) An optical disk player, comprising:  
an optical disk driver unit to read-out media content and a public key stored on an optical disk;

a network interface to download content associated with the read-out media content, the content residing on one or more computing devices distributed on a network; and

a control system to verify the authenticity of the downloaded content using the public key read-out from the optical disk before the read-out media content is played in coordination with the associated downloaded content.

21. (Previously presented) The optical disk player according to claim 20, wherein the control system detects whether the downloaded content is integral before verification, wherein said verification will not be executed if the downloaded content is detected to not be integral.

22. (Previously presented) The optical disk player according to claim 20, wherein the downloaded content is an application program.

23. (Previously presented) The optical disk player according to claim 22, wherein the application program is a JAVA language application program.

24. (Previously presented) The optical disk player according to claim 20, wherein the control system verifies the authenticity of downloaded content by performing asymmetric cryptography using the public key stored on the optical disk and corresponding to a private key used to encrypt the downloaded content.

25. (Previously presented) A method for playing an optical disk, comprising acts of:

reading-out media content and a public key stored on an optical disk;

downloading content associated with the read-out media content;

verifying the authenticity of the downloaded content using the public key read-out from the optical disk before allowing the read-out media content to be played in coordination with the associated downloaded content.

26. (Previously presented) The method according to claim 25, further comprising acts of:

detecting if the downloaded content is integral; and

executing the verifying act only if the downloaded content is detected to be integral.

27. (Previously presented) The method according to claim 25, wherein the coordination between the read-out media and downloaded content will not be established if the downloaded content is not

authenticated.

28. (Previously presented) The method according to claim 27, wherein the coordination between the read-out media and downloaded content will be established if the downloaded content is authenticated.

29. (Previously presented) The method according to claim 25, wherein the downloaded content is an application program.

30. (Previously presented) The method according to claim 29, wherein the application program is a JAVA language application program.

31. (Previously presented) The method according to claim 25, wherein verifying the authenticity of the downloaded content comprises an act of performing asymmetric cryptography using the public key read-out from the optical disk and a private key of the downloaded content.

32. (Currently amended) The method according to claim 25, wherein the optical disk comprises digital information stored thereon, the stored digital information comprising:

network address information that is used by the optical disk ~~playing-system-player~~ to download content for playing the optical disk; and

a public key that is used by the optical disk ~~playing-system~~ ~~player~~ to verify the authenticity of the downloaded content before playing the content ~~stored on the optical disk~~ in coordination with the ~~downloaded-content~~ stored on the optical disk.